L Number	Hits	Search Text	DB	Time stamp
-	62	vanstone-scott-a.in.	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/03/15 18:50
-	23	((multi$1party or multiparty or group or community or conference or multicast) near6 (key adj (agreement or exchange))) and @ad<19990719	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/03/16 15:08
-	0	((inter$1domain or multi$domain) near5 (key adj (agreement or exchange or management))) and @ad<19990719	USPAT; US-PGPUB; EPO; JPO; DERWENT; IBM_TDB	2004/03/16 14:34
-	1960	713/171;380/277-285,28-30.ccls. and @ad<19990719	USPAT; US-PGPUB	2004/03/17 12:21
-	54	(713/171;380/277-285,28-30.ccls. and @ad<19990719) and (group near3 ((public or private) adj key))	USPAT; US-PGPUB	2004/03/16 16:49
-	48	(713/171;380/277-285,28-30.ccls. and @ad<19990719) and ((generat$3 or comput$3 or calculat$3) with (group near2 key))	USPAT; US-PGPUB	2004/03/17 13:31
-	30	((713/171;380/277-285,28-30.ccls. and @ad<19990719) and ((generat$3 or comput$3 or calculat$3) with (group near2 key))) not ((713/171;380/277-285,28-30.ccls. and @ad<19990719) and (group near3 ((public or private) adj key)))	USPAT; US-PGPUB	2004/03/17 14:06
-	19	(380/44-47.ccls. and @ad<19990719) and ((generat$3 or comput$3 or calculat$3) with (group near2 key))	USPAT; US-PGPUB	2004/03/17 14:06
-	40	713/163;380/286.ccls. and @ad<19990719 and (group near2 key)	USPAT; US-PGPUB	2004/03/17 14:08

Search Results

Search Results for: **[(group key OR group session key OR group shared key OR group public key OR group private key)]**
Found **101** of **127,944 searched.**

Search within Results

GO > Advanced Search

> Search Help/Tips

Sort by: **Title** **Publication** **Publication Date** **Score** Binder

Results 1 - 20 of 101 **short listing**

Prev Page 1 2 3 4 5 6 Next Page

1 A survey of key management for secure group communication 100%
Sandro Rafaeli , David Hutchison
ACM Computing Surveys (CSUR) September 2003
Volume 35 Issue 3
Group communication can benefit from IP multicast to achieve scalable exchange of messages. However, there is a challenge of effectively controlling access to the transmitted data. IP multicast by itself does not provide any mechanisms for preventing nongroup members to have access to the group communication. Although encryption can be used to protect messages exchanged among group members, distributing the cryptographic keys becomes an issue. Researchers have proposed several different approach ...

2 Simple and fault-tolerant key agreement for dynamic collaborative groups 100%
Yongdae Kim , Adrian Perrig , Gene Tsudik
Proceedings of the 7th ACM conference on Computer and communications security November 2000

3 Secure group communications using key graphs 100%
Chung Kei Wong , Mohamed Gouda , Simon S. Lam
IEEE/ACM Transactions on Networking (TON) February 2000
Volume 8 Issue 1

4 Secure group communications using key graphs 100%
Chung Kei Wong , Mohamed Gouda , Simon S. Lam
ACM SIGCOMM Computer Communication Review , Proceedings of the ACM SIGCOMM '98 conference on Applications, technologies, architectures, and protocols for computer communication October 1998
Volume 28 Issue 4
Many emerging applications (e.g., teleconference, real-time information services,

h c g e cf e g e g e

pay per view, distributed interactive simulation, and collaborative work) are based upon a group communications model, i.e., they require packet delivery from one or more authorized senders to a very large number of authorized receivers. As a result, securing group communications (i.e., providing confidentiality, integrity, and authenticity of messages delivered between group members) will become a critical network ...

5 The architecture and performance of security protocols in the ensemble group communication system: Using diamonds to guard the castle 100%

ACM Transactions on Information and System Security (TISSEC) August 2001 Volume 4 Issue 3

Ensemble is a Group Communication System built at Cornell and the Hebrew universities. It allows processes to create *process groups* within which scalable reliable fifo-ordered multicast and point-to-point communication are supported. The system also supports other communication properties, such as causal and total multicast ordering, flow control, and the like. This article describes the security protocols and infrastructure of Ensemble. Applications using Ensemble with the extensions des ...

6 Authenticated group key agreement and friends 100%

Giuseppe Ateniese , Michael Steiner , Gene Tsudik

Proceedings of the 5th ACM conference on Computer and communications security November 1998

7 Batch rekeying for secure group communications 100%

Xiaozhou Steve Li , Yang Richard Yang , Mohamed G. Gouda , Simon S. Lam

Proceedings of the tenth international conference on World Wide Web April 2001

8 Reliable group rekeying: a performance analysis 100%

Yang Richard Yang , X. Steve Li , X. Brian Zhang , Simon S. Lam

ACM SIGCOMM Computer Communication Review , Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications August 2001 Volume 31 Issue 4

9 Cryptographic protocols/ network security: Efficient self-healing group key distribution with revocation capability 99%

Donggang Liu , Peng Ning , Kun Sun

Proceedings of the 10th ACM conference on Computer and communication security October 2003

This paper presents group key distribution techniques for large and dynamic groups over unreliable channels. The techniques proposed here are based on the self-healing key distribution methods (with revocation capability) recently developed by Staddon et al. [27]. By introducing a novel personal key distribution technique, this paper reduces (1) the communication overhead of personal key share distribution from $O(t^2 \log q)$ to $O(t \log q)$, (2) the communication overhead of self-healing key ...

10 Sensor networks: LEAP: efficient security mechanisms for large-scale distributed sensor networks 99%

Sencun Zhu , Sanjeev Setia , Sushil Jajodia

Proceedings of the 10th ACM conference on Computer and communication security October 2003

In this paper, we describe LEAP (Localized Encryption and Authentication Protocol), a key management protocol for sensor networks that is designed to support in-network processing, while at the same time restricting the security impact of a node

compromise to the immediate network neighborhood of the compromised node. The design of the protocol is motivated by the observation that different types of messages exchanged between sensor nodes have different security requirements, and that a single k ...

11 Secure key agreement for group communications 99%

Wen-Her Yang , Shiuh-Pyng Shieh
International Journal of Network Management November 2001
Volume 11 Issue 6

A secure key agreement protocol for group communications is proposed in this paper, which ensures the authenticity of group members and the privacy of group messages, and provides the properties of perfect forward and backward privacy. In a group session, the common key is collaboratively established by all participants, hence the overhead of key agreement is balanced among group members.

12 Group Key Management and Signatures: Formalizing GDOI group key management requirements in NPATRL 99%

Catherine Meadows , Paul Syverson
Proceedings of the 8th ACM conference on Computer and Communications Security November 2001

Although there is a substantial amount of work on formal requirements for two and three-party key distribution protocols, very little has been done on requirements for group protocols. However, since the latter have security requirements that can differ in important but subtle ways, we believe that a rigorous expression of these requirements can be useful in determining whether a given protocol can satisfy an application's needs. In this paper we make a first step in providing a formal understan ...

13 DG: a scalable approach for broadcasting data securely in wireless networks 98%

Aslihan Celik , Anindya Datta
Wireless Networks May 2003
Volume 9 Issue 3

This paper addresses the problem of providing *secure access control* in broadcast schemes in a wireless network. We consider an environment where clients subscribe to information objects sent via a broadcast onto a wireless network. In this context, a client should only be able to access its objects of interest for its subscription period, and the security system used must not be easily broken. Existing data broadcasting approaches fail to perform well with increased client loads. In this ...

14 A secure multicast protocol with copyright protection 98%

Hao-hua Chu , Lintian Qiao , Klara Nahrstedt , Hua Wang , Ritesh Jain
ACM SIGCOMM Computer Communication Review April 2002
Volume 32 Issue 2

We present a simple, efficient, and secure multicast protocol with copyright protection in an open and insecure network environment. There is a wide variety of multimedia applications that can benefit from using our secure multicast protocol, e.g., the commercial pay-per-view video multicast, or highly secure military intelligence video conference. Our secure multicast protocol is designed to achieve the following goals. (1) It can run in any open network environment. It does not rely on any sec ...

15 Algorithms for dynamic multicast key distribution trees 97%

Justin Goshi , Richard E. Ladner
Proceedings of the twenty-second annual symposium on Principles of distributed computing July 2003

Many secure group communication systems rely on a group key, which is a secret shared among the members of the group. Secure messages are sent to the group by encrypting them with the group key. Because group membership is dynamic, it becomes necessary to change the group key in an efficient and secure fashion when members join or leave the group. We present a series of algorithms for solving this problem based on 2--3 trees, where each internal node has degree 2 or 3. The algorithms attempt to ...

16 Secure protocol transformation via "expansion": from two-party to groups 97%

Alain Mayer , Moti Yung

Proceedings of the 6th ACM conference on Computer and communications security November 1999

The design of simple cryptographic protocols for elementary two-party (session oriented) tasks (such as entity authentication and key transport) has had a history (starting with [NS78]) where security has been quite evasive. Only recently we have seen protocol designs which are both provably secure and efficient Currently, much attention of the designers of network systems and services is directed towards group o ...

17 A scalable approach for broadcasting data in a wireless network 97%

Aslihan Celik , Anindya Datta

Proceedings of the 4th ACM international workshop on Modeling, analysis and simulation of wireless and mobile systems July 2001

This paper addresses the problem of providing *secure access control* in broadcast schemes in a wireless network. We consider an environment where clients subscribe to information objects sent via a broadcast onto a wireless network. In this context, a client should only be able to access its objects of interest for its subscription period, and the security system used must not be easily broken. Existing data broadcasting approaches fail to perform well with increased client loads. In th ...

18 Communication complexity of group key distribution 97%

Klaus Becker , Uta Wille

Proceedings of the 5th ACM conference on Computer and communications security November 1998

19 Group Key Management and Signatures: Practical forward secure group signature schemes 96%

Dawn Xiaodong Song

Proceedings of the 8th ACM conference on Computer and Communications Security November 2001

A group signature scheme allows a group member to sign messages anonymously on behalf of the group, while in case of a dispute, a designated entity can reveal the identity of a signature's originator. Group signature schemes can be used as a basic building block for many security applications such as electronic banking systems and electronic voting. Two important issues -- forward security and efficient revocation -- have not been addressed by prior schemes. We construct the first *forward-sec ...*

20 Security and Middleware Services: Efficient and secure keys management for wireless mobile communications 96%

Roberto Di Pietro , Luigi V. Mancini , Sushil Jajodia

Proceedings of the second ACM international workshop on Principles of mobile computing October 2002

This paper presents an efficient algorithm for the secure group key management of mobile users. The most promising protocols to deal with group key management are

those based on logical key hierarchy (LKH). The LKH model reduces to logarithmic size the resources needed: computation time, message exchanged, and memory space. In the framework of the LKH model, we present a new protocol LKH++ that outperforms the other proposed solutions in the literature. Such performance improvements are obtained ...

Results 1 - 20 of 101 **short listing**

Prev Page 1 2 3 4 5 6 Next Page

---

h c g e cf e g e g e